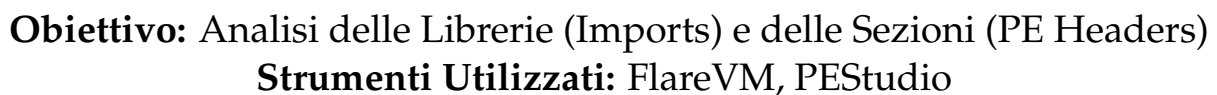


Target: File Eseguibile "notepad-classico.exe"

Data: 4 febbraio 2026



# Indice

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>Introduzione e Obiettivi</b>                   | <b>2</b> |
| 1.1      | Scenario . . . . .                                | 2        |
| 1.2      | Hash del File . . . . .                           | 2        |
| <b>2</b> | <b>Fase 1: Analisi delle Librerie (Imports)</b>   | <b>2</b> |
| 2.1      | Librerie Standard . . . . .                       | 2        |
| 2.2      | Funzioni Sospette e Flag Critici . . . . .        | 3        |
| <b>3</b> | <b>Fase 2: Analisi delle Sezioni (PE Headers)</b> | <b>3</b> |
| 3.1      | Anomalie Rilevate . . . . .                       | 3        |
| <b>4</b> | <b>Conclusioni e Classificazione</b>              | <b>4</b> |

# 1 Introduzione e Obiettivi

## 1.1 Scenario

L'obiettivo di questa attività è analizzare un file sospetto denominato notepad-classico.exe. Il file si presenta come un comune editor di testo, ma è sospettato di contenere funzionalità malevole nascoste. L'analisi è stata condotta in un ambiente isolato (FlareVM) utilizzando tecniche di analisi statica.

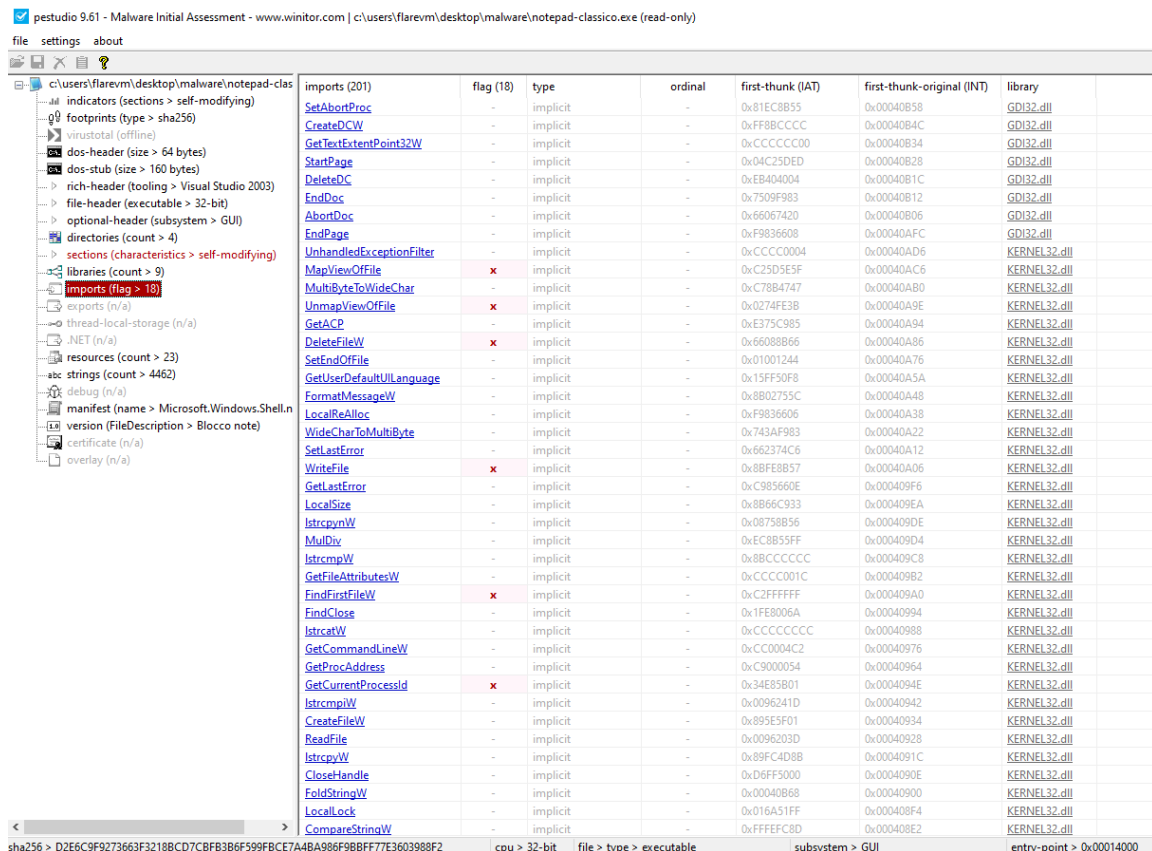
## 1.2 Hash del File

- **Nome File:** notepad-classico.exe
- **Contesto:** Esercitazione Malware Analysis

# 2 Fase 1: Analisi delle Librerie (Imports)

## 2.1 Librerie Standard

L'analisi preliminare tramite **PEStudio** mostra che il malware importa diverse librerie standard di Windows per simulare un comportamento legittimo. Sono presenti `comdlg32.dll` e `SHELL32.dll`, che forniscono le finestre di dialogo "Apri/Salva" e funzionalità di Drag & Drop, tipiche di un Notepad reale.



| imports (201)            | flag (18) | type     | ordinal | first-thunk (IAT) | first-thunk-original (INT) | library      |
|--------------------------|-----------|----------|---------|-------------------|----------------------------|--------------|
| SetAbortProc             | -         | implicit | -       | 0x81EC8B55        | 0x00040B58                 | GDI32.dll    |
| CreateDCW                | -         | implicit | -       | 0xFF8BCCCC        | 0x00040B4C                 | GDI32.dll    |
| GetTextExtentPoint32W    | -         | implicit | -       | 0xCCCCC000        | 0x00040B34                 | GDI32.dll    |
| StartPage                | -         | implicit | -       | 0x04C25DED        | 0x00040B28                 | GDI32.dll    |
| DeleteDC                 | -         | implicit | -       | 0xEB404004        | 0x00040B1C                 | GDI32.dll    |
| EndDoc                   | -         | implicit | -       | 0x7509F983        | 0x00040B12                 | GDI32.dll    |
| AbortDoc                 | -         | implicit | -       | 0x66067420        | 0x00040B06                 | GDI32.dll    |
| EndPage                  | -         | implicit | -       | 0xF9836608        | 0x00040AFC                 | GDI32.dll    |
| UnhandledExceptionFilter | -         | implicit | -       | 0xCCCC0004        | 0x00040AD6                 | KERNEL32.dll |
| MapViewOfFile            | x         | implicit | -       | 0xC25D5E5F        | 0x00040AC6                 | KERNEL32.dll |
| MultiByteToWideChar      | -         | implicit | -       | 0xC7884747        | 0x00040AB0                 | KERNEL32.dll |
| UnmapViewOfFile          | x         | implicit | -       | 0x0274FE3B        | 0x00040A9E                 | KERNEL32.dll |
| GetACP                   | -         | implicit | -       | 0xE375C985        | 0x00040A94                 | KERNEL32.dll |
| DeleteFileW              | x         | implicit | -       | 0x66088B66        | 0x00040A86                 | KERNEL32.dll |
| SetEndOfFile             | -         | implicit | -       | 0x01001244        | 0x00040A76                 | KERNEL32.dll |
| GetUserDefaultUILanguage | -         | implicit | -       | 0x15FF50F8        | 0x00040A5A                 | KERNEL32.dll |
| FormatMessageW           | -         | implicit | -       | 0x8B02755C        | 0x00040A48                 | KERNEL32.dll |
| LocalReAlloc             | -         | implicit | -       | 0xF9836606        | 0x00040A38                 | KERNEL32.dll |
| WideCharToMultiByte      | -         | implicit | -       | 0x743AF983        | 0x00040A22                 | KERNEL32.dll |
| SetLastError             | -         | implicit | -       | 0x662374C6        | 0x00040A12                 | KERNEL32.dll |
| WriteFile                | x         | implicit | -       | 0x8BFE8B57        | 0x00040A06                 | KERNEL32.dll |
| GetLastError             | -         | implicit | -       | 0xC985660E        | 0x000409F6                 | KERNEL32.dll |
| LocalSize                | -         | implicit | -       | 0x8B66C933        | 0x000409EA                 | KERNEL32.dll |
| IstrcpynW                | -         | implicit | -       | 0x08758B56        | 0x000409DE                 | KERNEL32.dll |
| MulDiv                   | -         | implicit | -       | 0xEC8B55FF        | 0x000409D4                 | KERNEL32.dll |
| IstrcmpW                 | -         | implicit | -       | 0x8BCCCCC         | 0x000409C8                 | KERNEL32.dll |
| GetFileAttributesW       | -         | implicit | -       | 0xCCCC001C        | 0x000409B2                 | KERNEL32.dll |
| FindFirstFileW           | x         | implicit | -       | 0xC2FFFFF         | 0x000409A0                 | KERNEL32.dll |
| FindClose                | -         | implicit | -       | 0x1FE8006A        | 0x00040994                 | KERNEL32.dll |
| IstrcatW                 | -         | implicit | -       | 0xCCCCCCCC        | 0x00040988                 | KERNEL32.dll |
| GetCommandLineW          | -         | implicit | -       | 0xC00004C2        | 0x00040976                 | KERNEL32.dll |
| GetProcAddress           | -         | implicit | -       | 0xC9000054        | 0x00040964                 | KERNEL32.dll |
| GetCurrentProcessId      | x         | implicit | -       | 0x34E85B01        | 0x0004094E                 | KERNEL32.dll |
| IstrcmpiW                | -         | implicit | -       | 0x0096241D        | 0x00040942                 | KERNEL32.dll |
| CreateFileW              | -         | implicit | -       | 0x895E3F01        | 0x00040934                 | KERNEL32.dll |
| ReadFile                 | -         | implicit | -       | 0x0096203D        | 0x00040928                 | KERNEL32.dll |
| IstrcpyW                 | -         | implicit | -       | 0x89FC4D8B        | 0x0004091C                 | KERNEL32.dll |
| CloseHandle              | -         | implicit | -       | 0xD6FF5000        | 0x0004090E                 | KERNEL32.dll |
| FoldStringW              | -         | implicit | -       | 0x00040B68        | 0x00040900                 | KERNEL32.dll |
| LocalLock                | -         | implicit | -       | 0x016A51FF        | 0x000408F4                 | KERNEL32.dll |
| CompareStringW           | -         | implicit | -       | 0xFFFFFEC8D       | 0x000408E2                 | KERNEL32.dll |

Figura 1: Librerie grafiche e di interfaccia utente.

## 2.2 Funzioni Sospette e Flag Critici

Approfondendo l'analisi della Import Address Table (IAT), PESTudio segnala numerosi **Red Flag** su funzioni critiche, in particolare nelle librerie `KERNEL32.dll` e `ADVAPI32.dll`.

Le funzioni più rilevanti identificate sono:

- **Gestione File e Memoria (KERNEL32.dll):**
  - `DeleteFileW`: Permette al programma di eliminare file dal disco. Comportamento anomalo per un editor di testo, spesso usato dai malware per cancellare le proprie tracce (self-deletion).
  - `MapViewOfFile` / `UnmapViewOfFile`: Utilizzate per mappare file in memoria. Queste API sono spesso sfruttate per tecniche di *Process Injection* (es. *Process Hollowing*).
- **Persistenza (ADVAPI32.dll):**
  - `RegCreateKeyW` / `RegSetValueExW`: Funzioni che permettono di scrivere nel Registro di Sistema. I malware le utilizzano per garantirsi la **persistenza**, aggiungendosi alle chiavi di avvio automatico (es. *Run keys*).
- **Monitoraggio (USER32.dll):**
  - `SetWinEventHook`: Può essere usata per intercettare input dell'utente (comportamento simil-keylogger).
  - `GetForegroundWindow`: Permette di sapere quale finestra l'utente sta utilizzando, tecnica usata dai banking trojan.

## 3 Fase 2: Analisi delle Sezioni (PE Headers)

L'analisi delle sezioni rivela anomalie strutturali che indicano che l'eseguibile è stato manipolato o "impacchettato" (Packed).

### 3.1 Anomalie Rilevate

Dalla tabella delle sezioni emergono i seguenti indicatori di compromissione:

1. **Duplicazione delle Sezioni:** Sono presenti sezioni con nomi duplicati (es. due sezioni `.text` e due `.rsrc`), indicando una possibile iniezione di codice post-compilazione.
2. **Permessi RWX (Sezione `.text` critica):** La sezione identificata come `section[3]` (`.text`) presenta permessi simultanei di **Scrittura (Write)** ed **Esecuzione (Execute)**.
  - Questa configurazione viola le policy di sicurezza standard (W^X).
  - Permette al codice di modificarsi durante l'esecuzione (Polimorfismo).
3. **Alta Entropia:** La stessa sezione presenta un valore di entropia pari a **6.428**. Sebbene non altissimo, combinato con il flag *Self-modifying*, suggerisce la presenza di codice offuscato o compresso per evadere l'analisi antivirus.

| property                    | value                      | value                      | value                      | value                      | value                       | value                      |
|-----------------------------|----------------------------|----------------------------|----------------------------|----------------------------|-----------------------------|----------------------------|
| section                     | section[0]                 | section[1]                 | section[2]                 | section[3]                 | section[4]                  | section[5]                 |
| name                        | .text                      | .data                      | .rsrc                      | .text                      | .idata                      | .rsrc                      |
| section > sha256            | 1813528212CAF80C7A8FEAF... | 87CB8581163F3AAB6623127... | 56074AE0754BC823C26E8C3... | 0033840D79E7586AE087A86... | 7420D4029AE4A33E573F7043... | C913461089289C2D4410DAE... |
| entropy                     | 6.214                      | 1.149                      | 5.421                      | 6.428                      | 5.439                       | 5.407                      |
| file > ratio (99.65%)       | 10.62 %                    | 0.71 %                     | 12.57 %                    | 61.59 %                    | 1.59 %                      | 12.57 %                    |
| raw-address (begin)         | 0x00000400                 | 0x00007C00                 | 0x00008400                 | 0x00011200                 | 0x0003CA00                  | 0x0003DC00                 |
| raw-address (end)           | 0x00007C00                 | 0x00008400                 | 0x00011200                 | 0x0003CA00                 | 0x0003DC00                  | 0x00046A00                 |
| raw-size (288256 bytes)     | 0x00007800 (30720 bytes)   | 0x00000800 (2048 bytes)    | 0x00008E00 (36352 bytes)   | 0x0002B800 (178176 bytes)  | 0x00001200 (4608 bytes)     | 0x00008E00 (36352 bytes)   |
| virtual-address (begin)     | 0x00001000                 | 0x00009000                 | 0x00008000                 | 0x00014000                 | 0x00040000                  | 0x00042000                 |
| virtual-address (end)       | 0x00008748                 | 0x0000ABA8                 | 0x00013DB4                 | 0x0003F6AC                 | 0x0004113E                  | 0x0004ADB0                 |
| virtual-size (292414 bytes) | 0x00007748 (30536 bytes)   | 0x00001BA8 (7080 bytes)    | 0x00008DB4 (36276 bytes)   | 0x0002B6AC (177836 bytes)  | 0x0000113E (4414 bytes)     | 0x00008DB0 (36272 bytes)   |
| characteristics             | 0x00000020                 | 0xC0000040                 | 0x40000040                 | 0xE0000020                 | 0xC2000040                  | 0x40000040                 |
| write                       | -                          | x                          | -                          | x                          | x                           | -                          |
| execute                     | x                          | -                          | -                          | -                          | -                           | -                          |
| share                       | -                          | -                          | -                          | -                          | -                           | -                          |
| self-modifying              | -                          | -                          | -                          | x                          | -                           | -                          |
| virtual                     | -                          | -                          | -                          | -                          | -                           | -                          |
| items                       |                            |                            |                            |                            |                             |                            |
| directory > import          | -                          | -                          | -                          | -                          | 0x00040000                  | -                          |
| directory > resource        | -                          | -                          | -                          | -                          | -                           | 0x00042000                 |
| directory > relocation      | -                          | -                          | -                          | 0x0003F698                 | -                           | -                          |
| directory > import-address  | 0x00001000                 | -                          | -                          | -                          | -                           | -                          |
| manifest                    | -                          | -                          | -                          | -                          | -                           | 0x00046712                 |
| version                     | -                          | -                          | -                          | -                          | -                           | 0x00046392                 |
| base-of-code                | 0x00001000                 | -                          | -                          | -                          | -                           | -                          |
| base-of-data                | -                          | 0x00009000                 | -                          | -                          | -                           | -                          |
| entry-point > location      | -                          | -                          | -                          | 0x00014000                 | -                           | -                          |

Figura 2: Analisi delle sezioni: evidenziati permessi RWX e flag self-modifying.

## 4 Conclusioni e Classificazione

Sulla base delle evidenze raccolte durante l'analisi statica, è possibile classificare il campione notepad-classico.exe come un **Trojan Spyware / Info Stealer**.

La classificazione è supportata dai seguenti fattori determinanti:

1. **Camuffamento (Trojan):** Il malware imita perfettamente un software legittimo (Blocco Note) nell'aspetto e nelle importazioni grafiche per ingannare l'utente.
2. **Funzionalità di Spionaggio (Spyware):** L'analisi delle importazioni rivela la capacità di monitorare la finestra attiva (GetForegroundWindow), accedere agli appunti di sistema (OpenClipboard) e agganciare gli eventi di input (SetWinEventHook). Queste sono caratteristiche tipiche dei malware progettati per il furto di credenziali o dati sensibili.
3. **Tecniche di Offuscamento (Packer/Dropper):** La struttura anomala del PE Header (sezioni RWX e flag *Self-modifying*) indica che l'eseguibile agisce come un *Dropper*: una volta avviato, decifra ed inietta il codice malevolo finale direttamente in memoria, rendendo più difficile la rilevazione da parte dei sistemi di sicurezza tradizionali.

In conclusione, il file rappresenta una minaccia ad alto rischio per la riservatezza dei dati e l'integrità del sistema.